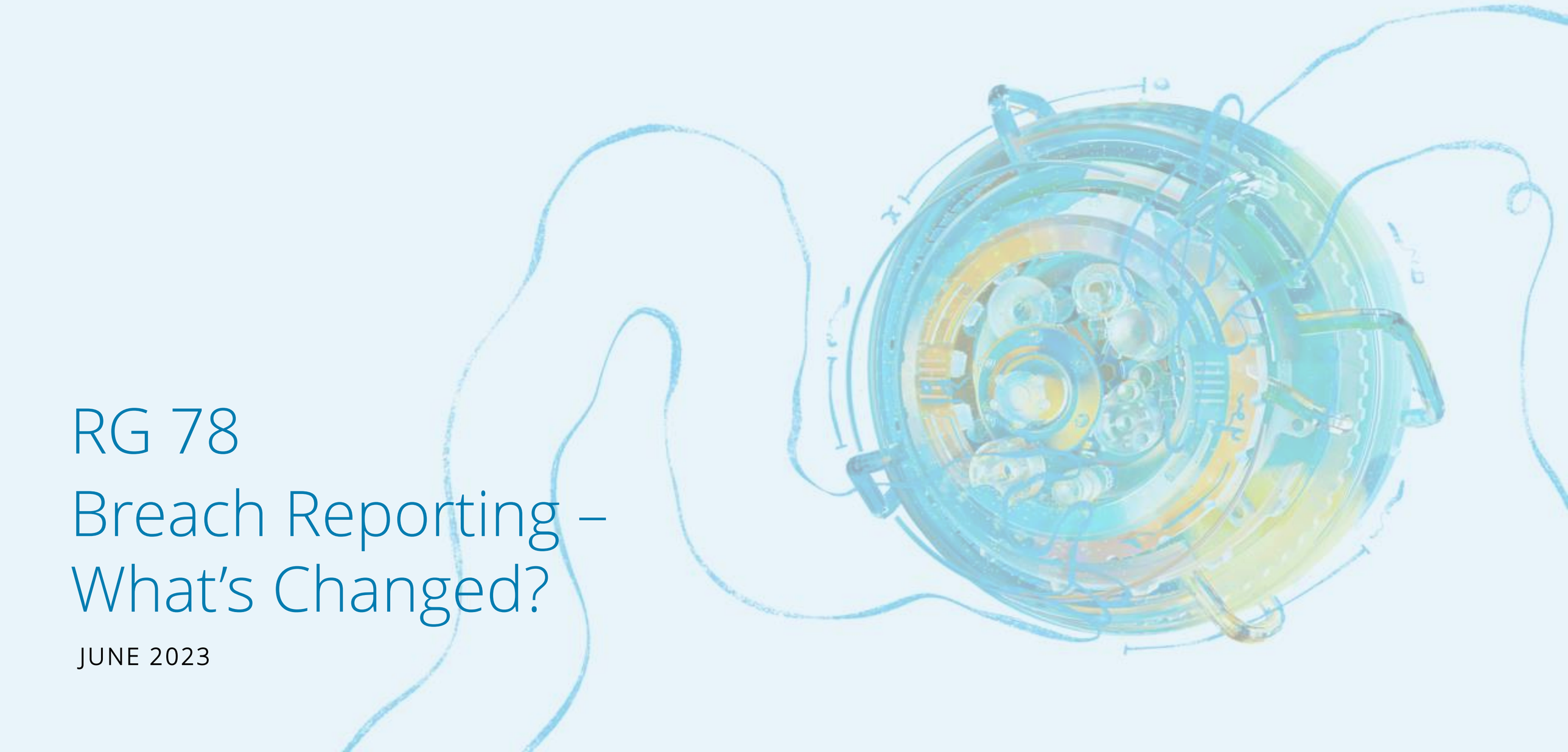
Deloitte.



RG 78
Breach Reporting – What's Changed?

JUNE 2023

Deloitte.

RG 78 Breach Reporting Updates

1 CONTEXT

In late 2022, ASIC consulted with industry stakeholders on improving *Regulatory Guide 78 – Breach Reporting by AFS licensees and credit licensees* ('RG 78').

On 27 April 2023, ASIC released the updated RG 78 along with an overview of the changes, which takes into account feedback from industry following the consultation. ASIC also outlined changes to its prescribed form for reporting, which commenced implementation from 5 May 2023. ASIC also advises that it will continue considering further items raised by industry.

This document sets out the key updates to RG 78, the impact and considerations for organisations and general insights we have gained through working with multiple organisations across the financial industry.

DELOITTE SURVEY RESULTS #1

68% of respondents use a Governance, Risk and Compliance ('GRC') system to record breaches, and only …

53% of respondents can automatically track relevant deadlines using their GRC system.

Source: Deloitte's internal survey of 65 AFS licensees across banking, superannuation, insurance, financial management, financial planning

2 RG 78 – WHAT'S UPDATED?

Reportable situation

- RG 78.112-117, Table 9
- RG 78.93-103
- Q1 and Q2 in Appendix 2

- **Grouping reportable situations.** Reportable situations may be grouped and reported in a single report if it meets both limbs of the 'grouping test' i.e. similar, related or identical conduct and the conduct has the same root cause.
- **Reportable situation description.** Description of reportable situations within the prescribed form is scalable depending on the nature and complexity of the breach.
- **'Similar' reportable situation**. In determining how far an organisation should 'look back' to identify if there has been a 'similar' reportable situation, consider whether there may be a repeat or broader systemic issue. Factors to consider include
  - the nature of the issue / breach,
  - the legislative provisions contravened,
  - the underlying root cause,
  - the compliance arrangements or controls involved and
  - the nature of client impact.
- **Date first discovered**. This is the date when a staff member or representative first discovered an incident is a suspected or possible reportable situation, not the date the incident was determined as a reportable situation.

Impact and considerations:
- *Update framework and policies to provide guidance on 'grouping.*
- *Review systems to allow and enable data capture to support 'grouping' and reporting to show the 'groupings' with insights for management information.*
- *Update policy / processes to appropriately interpret the date the organisation first discovered the reportable situation, to meet the 30-days reporting timeframe.*

Investigation

- Q6, Table 12 in Appendix 2

- **Investigation trigger**. Investigation triggers are defined and reference to the guide is embedded within the prescribed from.
- **Investigation completion**. An investigation is complete after the licensee has determined the root cause(s), identified all affected clients and identified all instances of the reportable situation.

Impact and considerations:
- *Revisit investigation triggers to ensure alignment with the ASIC definitions.*
- *Update policies / processes where required to align with risk metrics.*
- *Accurate identification of investigation triggers can support with understanding around effectiveness of controls to identify incidents, and whether the control environment can be enhanced.*

Root cause

- Q4, Table 11 in Appendix 2

- **Root cause category**. Root cause category options are defined and reference to the guide is embedded within the prescribed form.

Impact and considerations:
- *Consider aligning root cause definitions with ASIC's definitions, including ensuring root cause analysis processes are fit for purpose and staff are provided appropriate guidance on the definitions.*
- *Alignment is intended to provide increased clarity and consistency in selecting the root cause category options when reporting breaches.*

Client impact

- Q5 in Appendix 2

- **Clients affected and loss**. 'Genuine estimates' must be provided on the total number of clients affected and client loss based on the facts available at the time of reporting. Organisations should not use a 'nil' placeholder when reporting.

Impact and considerations:
- *As part of investigations, take appropriate steps to collect and assess the relevant information upfront to estimate the client impact within the 30-days timeframe.*
- *Prioritise incidents / breaches and make an earlier determination whether a customer remediation program of work is required to provide appropriate and timely compensation.*

Reporting updates, withdrawals or correction

- Q3 and Q7, Table 13 in Appendix 2

- **Updates**. Updates must be provided: every six months; where there are material changes to the nature, impact or extent of the reportable situation; or, when the investigation, rectification of root cause(s) and consumer remediation is completed.
- **Withdraw or correction**. There are limited circumstances in which organisations can withdraw or correct a report, including where there are material factual errors; a change is required to a field that has been greyed out; additional or more accurate information is identified.

Impact and considerations:
- *Use system support to track reporting timeframes.*
- *Implement system flags / notifications to update, withdraw or correct reports every six months or when material changes are made within the incident record.*
- *More rigour in monitoring and managing incidents is required to ensure appropriate updates are provided on reported breaches.*

Deloitte.

RG 78 Breach Reporting Updates

3 HOW WE CAN SUPPORT YOU

The following outlines **how we can support you** with addressing the updated RG requirements in relation to your incident management and breach reporting process.

STREAMLINE AND AUTOMATE

This involves removing process inefficiencies and using the GRC system to automate some activities within the incident management lifecycle to create a streamlined process for breach reporting. For example:

- ❑ Developing triaging criteria to adopt a risk-based approach to assessing breaches.
- ❑ Analysing historical breach data and creating a list of common 'deemed significant breaches' to support with triaging incidents.
- ❑ Refreshing business rules to support with automating activities within the GRC system in line with the required timeframes.
- ❑ Helping you redesign the GRC system to support with accurate and complete data capture.
- ❑ Reviewing and providing recommendations to uplift investigation processes, including root cause analysis.
- ❑ Helping you operate efficiently and meet regulatory timeframes through a managed services arrangement or outsourcing support to address fluctuating volumes.

ALIGN AND ENHANCE

This involves enhancing data quality captured within the GRC system to support with effective investigation (including root cause analysis and identification of potentially systemic issues) and reporting breaches.

- ❑ Developing minimum standards with relevant examples for information capture within the GRC system.
- ❑ Conducting a data inventory to source, collate and analyse data from verified internal sources to identify potentially systemic issues, with a data reliability analysis conducted in parallel.
- ❑ Helping you explore consolidating datasets and ability to upload to ASIC using a breach reporting solution, co-ordinate reporting and industry insights.

GUIDE AND EMPOWER

This involves providing guidance and training to uplift organisational capability and empower staff to effectively and efficiently manage incidents and breaches.

- ❑ Developing or refreshing staff training based on the updated requirements and better industry practice, including to support the reinforcement of a culture which links incident management and breach reporting with positive customer outcomes.
- ❑ Providing scenario-based learning to support staff with identifying, managing and resolving incidents / breaches.
- ❑ Helping you with responding and engaging with the regulator.

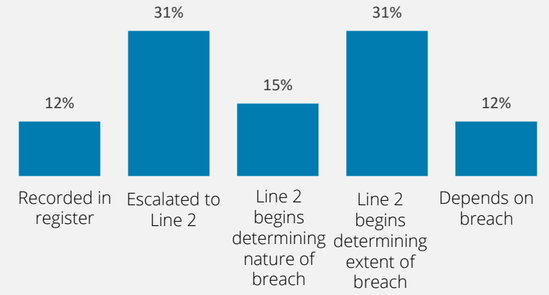
ANALYSE AND UNDERSTAND

This involves having processes and controls in place to identify, analyse and understand incidents and breaches, including emerging issues within the business.

- ❑ Helping you design a systemic issues operating model.
- ❑ Reviewing end-to-end process and identifying control gaps or enhancements, including opportunities to implement detective controls.
- ❑ Sharing insights on local and international developments on emerging and identified systemic issues, for organisations to test (If applicable).
- ❑ Supporting you with analysing impact of breaches and remediating impacted customers, including determining financial loss.

DELOITTE SURVEY RESULTS #2

When does the 30 days' 'investigation' begin?



Source: Deloitte's internal survey of 65 AFS licensees across banking, superannuation, insurance, financial management, financial planning

CONTACT US

John Weaver
Partner
Governance, Regulation and Conduct
joweaver@deloitte.com.au

Lingwei Low
Partner
Governance, Regulation and Conduct
linlow@deloitte.com.au

Sweta Maira
Partner
Audit & Assurance Analytics
smaira@deloitte.com.au

Deloitte.